

IN THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

I, John Gillette, Special Agent (“SA”) of the United States Secret Service (“USSS”),
Cleveland, OH, Field Office, hereinafter referred to as Affiant, being duly sworn on oath, hereby
depone and state as follows:

INTRODUCTION

1. Affiant is an investigative or law enforcement officer of the United States within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), as a SA of the USSS. Affiant is empowered to conduct investigations of and to make arrests for federal offenses, *see* 18 U.S.C. § 3056. Affiant has been employed by the USSS since June 9, 2011, and has been assigned to the investigation of financial crimes in the Cleveland, OH District. Affiant has been charged with the investigation of federal crimes involving identity fraud, credit card fraud, check fraud, bank and wire fraud, and the manufacturing, possession and passing of counterfeit United States currency in the Northern District of Ohio. At all times during the investigation described in this affidavit, Affiant has acted in an official capacity as a SA of the USSS. Prior to joining the USSS, Affiant was a Uniformed Division Officer with the USSS in Washington, DC. While in that position, Affiant was charged with enforcing Washington DC laws and Federal Code, protection of persons and facilities at the White House and Naval Observatory branch, and training of new recruits and operational personnel at the USSS training center in Beltsville, MD.

2. Affiant has participated in all of the usual methods of investigation, including, but not limited to, physical surveillance, the questioning of witnesses, and the analysis of evidence. Affiant has participated in the execution of arrest and search warrants resulting in the seizure of criminally derived property, including but not limited to, monetary instruments.

3. This affidavit is offered in support of a warrant to search the electronic contents of the following three laptop computers, two cellular telephones, one computer hard drive, one SIM Card, and two USB storage devices:

- a. Acer, Model N15Q9, laptop computer, Serial Number: NXGHJAA00274100C2C7600,
- b. Dell, Model Latitude E5570, laptop computer, Serial Number: D4L53G2,
- c. Motorola, Model XT1766, cellular telephone, Serial Number: 256691544209590567,
- d. HP, Model dv6910us, laptop computer, Serial Number: CNF8283D64,
- e. Motorola, Model XT1609, cellular telephone, Serial Number: 354142074026156,
- f. Western Digital, Hard Disk Drive, Serial Number: WMAV92999907,
- g. Communication Devices-Portable/SIM card, Serial Number: 8914800003614676406,
- h. Micro SD, Computer Equipment Storage Device, Model USB 2.0, and
- i. PNY, Computer Equipment Storage Device, Model 8GB.

Items a through i above shall hereinafter be referred to as the "Target Devices." The above target devices are currently listed on attached property receipts 2032019CE000039, 2032019CE000040, 2032019CE000041, 2032019CE000042, 2032019CE000043, 2032019CE000044, 2032019CE000045, and 2032019CE000046, respectively; items g and h are both listed on property receipt 2032019CE000045. The above items are to be searched for content including, but not limited to: contact lists and/or address books, call logs, digital pictures, digital video, digital media, text messages, audio files, e-mails, personal calendars, downloaded internet content, internet protocol addresses ("IP addresses"), and Global Positioning System ("GPS") points.

4. The statements contained in this affidavit are based in part on information developed by other SAs of the USSS and officers and detectives of Portage County Sheriff's Office who aided in the investigation. Unless otherwise noted, whenever in this affidavit your Affiant asserts that a statement was made, the information regarding that statement was provided by another law enforcement officer or an investigator (who may have had either direct or hearsay knowledge of the statement) to whom your Affiant has spoken or whose report your Affiant has read and reviewed. Likewise, any information pertaining to vehicles and registrations, personal data on subjects, and record checks, has been obtained through the Law Enforcement Automated Data System (LEADS), various state driver's license motor vehicle records, online database searches or the National Crime Information Center (NCIC) computers, and various open source databases such as LexisNexis.

5. Because this affidavit is being submitted for the limited purpose of supporting the application in this matter, Affiant has not included each and every fact known to him concerning this investigation. Affiant has set forth only the facts that he believes are necessary to establish the probable cause for the issuance of the search warrant sought.

BACKGROUND REGARDING CELLULAR TELEPHONES, PORTABLE MEDIA
PLAYERS, GPS NAVIGATION DEVICES, TABLET DEVICES, AND LAPTOPS

6. Through Affiant's training and experience, Affiant is aware of the following:
 - a. Cellular telephones allow users to connect to other users of cellular telephones through voice, e-mail, and text messaging.
 - b. Cellular telephones have the capability of using GPS to display their current locations. A cellular telephone, when functioning as a GPS navigation device, often records the locations where it has been.

- c. Cellular telephones have the capability to connect to the internet through “wi-fi” or a cellular telephone carrier’s network. An IP address is a unique numeric address used by devices on the internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). An IP address allows internet traffic to be directed properly from its source to its destination.
- d. Cellular telephones have the capability to download digital pictures, digital video, digital media, and audio files.
- e. Cellular telephones will often store contact lists or “address books” and personal calendars for users.
- f. Individuals involved in criminal activity utilize cellular telephones to facilitate crimes. Specifically, your Affiant is aware that individuals involved in criminal activity utilize cellular telephones, whether through telephone conversations or text messages, as a medium to communicate with co-conspirators during the planning and commission of crimes.
- g. Those involved in criminal activity frequently keep names and phone numbers of co-conspirators in the electronic contact list or address book utility located within the cellular telephone device.
- h. Individuals involved in criminal activity will frequently disconnect the battery from their cellular telephone in attempts to avoid detection by law enforcement.
- i. Electronic devices can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic

tools.

- j. A GPS navigation device uses the Global Positioning System to display its current location. The device often contains records of the locations where the device has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. A GPS navigation device uses 24 Navstar satellites orbiting the Earth. The satellites transmit radio signals, corresponding with the time and identification of the particular satellite, to Earth. When a GPS antenna receives a signal from at least four Navstar satellites, a computer connected to that antenna can mathematically calculate the antenna's location, including latitude, longitude, and sometimes altitude, with a high level of precision.

7. Based on knowledge, training, and experience, Affiant knows that electronic devices can store information for long periods of time. Similarly, electronic devices typically store data regarding the device's Internet activity for a period of time. This data can sometimes be recovered from the device using forensics tools.

8. There is probable cause to believe that data that were once stored on the Target Devices may still be stored there, for at least the following reasons:

- a. Based on knowledge, training, and experience, Affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

9. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct

evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Target Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Target Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

10. Nature of examination. Based on the foregoing, and consistent with Federal Rule of Criminal Procedure Rule 41(e)(2)(B), this applications seeks the issuance of a warrant that would permit the examination of the Target Devices consistent with the warrant. Forensic examination of Target Devices to search for artifacts associated with the production and distribution of counterfeit currency. This application seeks the issuance of a warrant authorizing forensic search and seizure techniques, including, but not limited to, computer-assisted scans of the entire target devices that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

11. Manner of execution. Because this warrant seeks only permission to examine Target Devices, which are already in the possession of law enforcement, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, Affiant submits there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

12. Examining data stored on devices of the types described above can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

13. Based upon Affiant's training and experience, and after reviewing the evidence, which is set forth in detail below, probable cause exists to believe that the electronic data maintained in the Target Devices contains information regarding the manufacture of counterfeit currency that occurred on or around April 20, 2018. Thus, as set forth herein, there is probable cause to believe that within the Target Devices, there exist fruits, evidence, or instrumentalities of violations of Title 18, United States Code, Sections 471 and 472.

FACTS AND CIRCUMSTANCES REGARDING PROBABLE CAUSE AS TO
VIOLATIONS OF 18 U.S.C. §§ 471 AND 472

14. On April 20, 2018, Individual 1, whose identity is known to Affiant, reported to the Portage County Sheriff's Office ("PCSO") in Ravenna, Ohio that she had recently sold a "go-kart" to JUSTIN SMITH and that SMITH paid for the "go-kart" in part with currency that Individual 1 believed to be counterfeit. Individual 1 advised PCSO that she had agreed, using the website and cellular telephone application "Offer Up," to sell to SMITH a go-kart in her possession for \$345.00. Individual 1 also indicated that she met with SMITH on or about April 20, 2018 in Ravenna, Ohio to execute the agreed-upon sale. SMITH made payment with 13 twenty dollar bills of United States currency, and after receiving the payment, Individual 1

permitted SMITH to take possession of the go-kart, which SMITH drove away.

15. After the transaction, Individual 1 went to an automated teller machine (“ATM”) to deposit the money she had received from SMITH. The machine would not accept two of the 13 twenty dollar bills that Individual 1 received from SMITH. Individual 1 stated to PCSO that she tested the two twenty dollar bills at home using a counterfeit currency marker, which serves as a counterfeit bill detector, and the test indicated that the bills were counterfeit. Individual 1 also stated to PCSO that the texture of the bills felt different than normal currency and that the margins of the bills appeared to be cut on an angle.

16. Individual 1 also provided PCSO investigators with the transcript of her conversation with SMITH on the Offer Up application relating to the sale of the go-kart.

17. On or about April 23, 2018, PCSO investigators made contact with SMITH at his residence at 4289 Sandy Lake Road in Rootstown Township, Ohio. SMITH’S sister, who is known to law enforcement, was present at the residence. She informed PCSO investigators that she was present with SMITH during the transaction and that remembered the price as “three forty something.” SMITH stated to PCSO investigators that the price of the go-kart was \$350.00 and that he paid with hundred dollar bills and fifty dollar bills. SMITH also stated that he did not make payment to Individual 1 using twenty dollar bills.

18. On or about April 25, 2018, PCSO investigators searched and reviewed counterfeit currency already in the possession of the PCSO as evidence in other matters. Amongst that currency already in the possession of the PCSO, PCSO investigators discovered a counterfeit twenty dollar bill with the same serial number as the two twenty dollar bills provided to the PCSO by Individual 1. That counterfeit twenty dollar bill was recovered by PCSO after it was used on or about April 20, 2018, at a gas station located approximately one mile from

SMITH's residence. Gas station employees were not able to provide a description of the individual who used the counterfeit the counterfeit twenty dollar bill.

19. On or about April 25, 2018, PCSO investigators spoke with other PCSO investigators who had previous contact with SMITH. It was learned from those PCSO investigators that during a previous parole search in 2016 at SMITH's residence at 4289 Sandy Lake Road, counterfeit was observed in plain view. A search warrant was subsequently obtained for the residence, and a search of the residence resulted in the recovery of numerous counterfeit twenty dollar bills, paper used to print counterfeit currency, and bags of paper clippings with counterfeit currency markings. Several of the items had been recovered in SMITH's bedroom. During an interview with SMITH subsequent to the execution of the search warrant, SMITH stated to investigators that he permitted multiple individuals to manufacture counterfeit currency in the basement of his residence and that they were using the counterfeit currency for the purchase of illegal controlled substances.

20. Based on the probable cause above, PCSO investigators obtained and executed a search warrant on April 27, 2018 at SMITH's residence at 4289 Sandy Lake Road in Rootstown as part of an investigation into the manufacture and uttering of counterfeit U.S. currency.

FACTS AND CIRCUMSTANCES REGARDING PROBABLE CAUSE AS TO
USE OF LAPTOPS, CELLULAR TELEPHONES, HARD DRIVE, SIM CARD, AND USB
STORAGE DEVICES TO FURTHER THE MANUFACTURE AND UTTERING OF
COUNTERFEIT U.S. CURRENCY

21. During the execution of the aforementioned search warrant on April 27, 2018 at SMITH's residence at 4289 Sandy Lake Road, Smith was observed by PCSO investigators attempting to flee from the rear of the residence.

22. During his apprehension, SMITH admitted to being in possession of methamphetamine. From SMITH's person, methamphetamine and as well as drug paraphernalia were recovered, and SMITH was placed under arrest.

23. During the execution of the search warrant at 4289 Sandy Lake Road, PCSO found and recovered the TARGET DEVICES, listed below, in SMITH'S bedroom within the residence:

- a. Acer, Model N15Q9, Laptop Computer, Serial Number:
NXGHJAA00274100C2C7600
- b. Dell, Model Latitude E5570, Laptop Computer, Serial Number: D4L53G2
- c. HP, Model dv6910us, Laptop Computer, Serial Number: CNF8283D64
- d. Motorola, Model XT1766, cellular telephone, Serial Number:
256691544209590567
- e. Motorola, Model XT1609, Cellular Telephone, Serial Number: 354142074026156
- f. Western Digital, Hard Disk Drive, Serial Number: WMAV92999907
- g. Communication Devices-Portable/Sim Card, Serial Number:
8914800003614676406
- h. Micro SD, Computer Equipment Storage Device, Model USB 2.0
- i. PNY, Computer Equipment Storage Device, Model 8GB

24. During the execution of the search warrant the following items were also found and recovered in SMITH's bedroom:

- a. Paper cutter
- b. Ink cartridges for an Hewlett Packard printer
- c. Photo glass
- d. Resume Paper

- e. Counterfeit \$20.00 US Currency
- f. Copier
- g. Printer – Hewlett Packard
- h. Cutting sheet
- i. Prop money \$10.00's, \$50.00's, and \$100.00's
- j. Counterfeit Marking Pens
- k. HD Photosmart Printer
- l. Counterfeit US Currency

25. Based on my training, experience, and knowledge, I know that many of the above items are often used in the manufacture of counterfeit currency and that multiple of the above items being discovered in the same location is often evidence of a counterfeit currency manufacturing operation. Resume paper is commonly used by counterfeiters to alter the feel of counterfeit currency to more closely resemble that of genuine US currency. Individuals who are manufacturing counterfeit currency also commonly use copiers and printers to scan genuine US currency, save and alter the images, and print counterfeit bills. Individuals involved in the manufacture of counterfeit currency would then use items like a paper cutter and cutting sheets to accurately cut the printed counterfeit bills from the larger sheets of paper. Counterfeit marking pens are sold legally, and often used to businesses who use the pens to test and identify currency that is received from customers. Manufacturers of counterfeit currency often use those same counterfeit marking pens to test the quality of the counterfeit currency the manufacturer is able to produce.

26. PCSO discovered that the Dell Latitude E5570 bearing serial number D4L53G2 had been reported stolen to the Kent State University Police Department, and an arrest warrant

was obtained to charge SMITH in Ohio state court with receiving stolen property, in violation of Title 29, Ohio Revised Code § 2913.51.

A. Interview of Justin Smith

27. After the execution of the arrest warrant, SMITH was advised of his Miranda rights, including his right to remain silent. On or about May 3, 2018, SMITH agreed to speak with PCSO investigators.

28. SMITH admitted to PCSO investigators that “doubled his paychecks,” and he explained to PCSO investigators that whenever he received “hard earned money” in a two week paycheck, he would then manufacture that same amount of counterfeit currency to effectively double his paycheck. SMITH stated he recalled printing approximately \$8,000.00, and he added that this estimate did not include counterfeit bills that were “scrapped.”

29. SMITH also admitted to PCSO investigators that there had been a large container of counterfeit money in the shed on his property at 4289 Sandy Lake Road and that investigators did not locate during the execution of the search warrant. SMITH stated he later destroyed the counterfeit currency that investigators did not locate in a “big ass fire”.

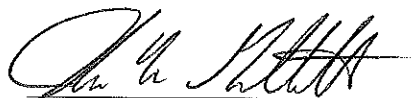
C. Current Location of Target Devices

30. On January 10, 2019 the Target Devices were retrieved from evidence in Portage County Justice Center by SA Gillette and transferred them to Cleveland USSS Evidence. The Target Devices remain in Cleveland USSS Evidence today.

CONCLUSION

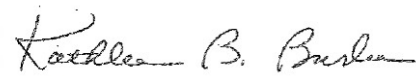
31. Based on the foregoing facts, your Affiant respectfully submits that there is probable cause to believe that within the TARGET DEVICES, identified in detail in Attachment A, there exists fruits, evidence, and instrumentalities of violations of Title 18, United States Code, §§ 471 and 472.

32. Your Affiant respectfully requests that the Court issue a search warrant for the Target Devices to be searched for said fruit, evidence and instrumentalities, identified in detail in Attachment B.



John W. Gillette, Special Agent
United States Secret Service
Cleveland, Ohio

This affidavit was sworn to by the affiant by telephone after a PDF was transmitted by email, per Crim R. 41(d)(3)



Kathleen B. Burke, U.S. Magistrate Judge

Dated: 4/5/2019